AMENDMENTS TO THE CLAIMS:

The following listing of claims will replace all prior versions, and listings, of claims in the captioned Application:

Listing Of Claims:

Claim 1 (currently amended): A method for authenticating transferred data between a sender computer and a receiver computer over an open network, the method comprising the steps of:

establishing a first secure transmission of data between the sender computer and the receiver computer;

transmitting selected authentication information including at least one token and a checksum value from the sender computer to the receiver computer during the first secure transmission so as to allow the sender computer to authenticate itself, the number of tokens being set to a variable N where N defines a selected number of additional transmissions and each token is a unique identifier;

transmitting an acknowledgment from the receiver computer to the sender computer, upon successful receipt and processing of the first transmission by the receiver computer;

establishing at least one additional transmission of data between the sender computer and the receiver computer;

transmitting the data and the at least one token from the sender computer to the receiver computer during the at least one additional transmission;

comparing the at least one token transmitted from the sender computer during the [at least one] additional transmission to each of the [at least one] token(s) transmitted from the sender computer during the [first secure] one or more previous transmission(s) to determine whether the most recent additional transmission is authentic; and

[each time a first] establishing a second secure transmission [is performed,] during which the sender computer transmits to the receiver computer a second selected value of N, [and] N number of tokens and a second checksum value to be used to authenticate the sender computer.

Claim 2 (previously presented): The method set forth in claim 1, wherein the at least one token comprises a preselected number of tokens.

Claim 3 (previously presented): The method set forth in claim 2, wherein the number of at least one transmissions corresponds to the preselected number of tokens.

Claim 4 (previously presented): The method set forth in claim 2, wherein the number of at least one transmissions is greater than the preselected number of tokens.

Claim 5 (previously presented): The method set forth in claim 2, wherein the number of at least one transmissions is less than the preselected number of tokens.

Claim 6 (previously presented): The method set forth in claim 1, wherein the at least one additional transmission is conducted over an unsecure or open connection.

Claim 7 (previously presented): The method set forth in claim 1, wherein the first secure transmission is encrypted.

Claim 8 (previously presented): The method set forth in claim 1, wherein the at least one additional transmission is sent in plaintext.

Claim 9 (previously presented): The method set forth in claim 5, wherein the at least one additional transmission is sent in plaintext.

Claim 10 (previously presented): The method set forth in claim 2, wherein the first secure transmission is encrypted.

Claim 11 (previously presented): The method set forth in claim 3, wherein the at least one additional transmission is sent in plaintext.

Claim 12 (previously presented): The method set forth in claim 1, further comprising the steps of transmitting a checksum value during the first transmission and having the receiver verify that the checksum value is accurate by comparing the transmitted value to a checksum value generated using a similar checksum algorithm.

Claim 13 (previously presented): The method set forth in claim 10, wherein the transmitted checksum value is based upon checksum values transmitted during previous transmissions.

Claim 14 (currently amended): A method for securely transferring data between a client computer and a server over an open network, the method comprising the steps of:

establishing a first secure transmission between the client computer and the server which is encrypted;

transmitting selected authentication information including a preselected number of tokens and a checksum value from the client computer to the server during the first secure transmission so as to allow the sender computer to authenticate itself, the number of tokens being set to a variable N where N defines a selected number of additional transmissions and each token is a unique identifier;

transmitting an acknowledgment from the server to the client computer, upon successful receipt and processing of the first transmission by the client computer;

establishing additional transmissions between the client computer and the server corresponding to the preselected number of tokens N;

transmitting the data [and], one of the preselected tokens and the checksum value from the client computer to the server during each additional transmission;

during each additional transmission, comparing the token transmitted from the client computer to the server during [the] such additional transmission to the corresponding token transmitted during the first secure transmission to determine whether the additional transmission is authentic; and

[each time a first] establishing a second secure transmission [is performed,] during which the client computer transmits to the server a second selected value of N, [and] N number of tokens and a second checksum value to be used to authenticate the client computer.

Claim 15 (previously presented): The method set forth in claim 14, wherein the additional transmissions are sent in plaintext.

Claim 16 (previously presented): The method set forth in claim 14, further comprising the steps of transmitting a checksum value during the first transmission and having the receiver computer verify that the checksum value is accurate by comparing the transmitted checksum value to a checksum value generated using a similar algorithm.

Claim 17 (previously presented): The method set forth in claim 16, wherein the transmitted checksum value is based upon checksum values transmitted during previous transmissions during this transaction.

Claim 18 (previously cancelled).

Claim 19 (previously presented): The method set forth in claim 1, wherein the additional transmissions are variable and adaptively selected, at least in part, based upon the performance overhead of the system.

Claim 20 (previously presented): The method set forth in claim 1, wherein the additional transmissions are variable and adaptively selected, at least in part, based upon monitored conditions.

Claim 21 (previously cancelled).

Claim 22 (previously presented): The method set forth in claim 23, wherein the algorithm is a statistical averaging algorithm.

Claim 23 (currently amended): A method for authenticating transferred data between a sender computer and a receiver computer over an open network, the method comprising the steps of:

establishing a first secure transmission of data between the sender computer and the receiver computer;

transmitting selected authentication information including at least one token and a checksum value from the sender computer to the receiver computer during the first secure transmission so as to allow the sender computer to authenticate itself, the number of tokens being set to a variable N where N defines a selected number of additional transmissions and each token is a unique identifier;

transmitting an acknowledgement from the receiver computer to the sender computer, upon successful receipt and processing of the first transmission by the receiver computer;

establishing at least one additional transmission of data between the sender computer and the receiver computer;

transmitting the data and the at least one token from the sender computer to the receiver computer during the at least one additional transmission;

comparing the at least one token transmitted from the sender computer during the [at least one] additional transmission to each of the [at least one] token(s) transmitted from the sender computer during the [first secure] one or more previous transmission(s) to determine whether the most recent additional transmission is authentic; and

[each time a first] establishing a second secure transmission [is performed,] during which the sender computer transmits to the receiver computer a second